https://doi.org/10.31891/2219-9365-2023-76-17
УДК 004.056

КОРЧИНСЬКИЙ Володимир
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0000-0003-3972-0585
e-mail: vkadkorchin@ukr.net
ТАРАСЕНКО Ірина
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0009-0009-5736-5979
tarasenkoirina1967@gmail.com
БЄЛОВА Юлія
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0000-0002-0631-7282
e-mail: bilovaulia@gmail.com
РАЦИБОРИНСЬКИЙ Сергій
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0009-0000-2513-8442
e-mail: raciborinskij@ukr.net
АКАЄВ Олександр
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0009-0008-4336-2331
e-mail: dobrodeetel@gmail.com

АТАКИ НА ОСНОВІ BADUSB

У роботі розглянуто загальні положення атаки на основі BadUSB. Дана атака використовує вразливості у USB пристроях для впровадження шкідливих програм та атак на комп'ютерні системи. Концепція BadUSB базується на зміні програмного забезпечення контролера USB пристрою, дозволяючи зловмисникам змінювати функціональність пристрою. Наприклад, імітувати різні типи пристроїв, такі як клавіатура, миша, мережевий адаптер тощо, для виконання різноманітних шкідливих дій. Зловмисники/хакери можуть використовувати BadUSB для запуску шкідливого коду на комп'ютері-хості. Це дозволяє перехоплювати дані, здійснювати віддалене керування, виконувати шкідливі команди та інші шкідливі операції на зараженій системі. Атака BadUSB може бути використана для здійснення широкого спектру атак, обходячи традиційні методи захисту. Одним із основних методів захисту від атак BadUSB є обмеження доступу до USB портів та використання механізмів контролю доступу для пристроїв, які під'єднуються до комп'ютера. Також важливо оновлювати програмне забезпечення USB пристроїв. Для зменшення ризиків необхідно постійно оновлювати системи безпеки та впроваджувати заходи контролю з метою запобігання можливих атак через USB інтерфейс. BadUSB визначається як загроза, яка вимагає уваги та подальших досліджень для розробки більш ефективних методів виявлення та захисту від подібних атак, зберігаючи при цьому функціональність USB-пристроїв. Однак BadUSB не обмежується лише імітацією периферійних пристроїв. Відомі випадки даної атаки, що спрямовані на USB-накопичувачі та інші пристрої, які використовують USB-підключення. Зловмисники/хакери можуть вставляти шкідливий код або виправляти програмне забезпечення на цих пристроях, щоб виконати атаки, спрямовані на викрадення чи видалення конфіденційної інформації. Захист від BadUSB вимагає комплексного підходу, включаючи вдосконалення апаратної та програмної безпеки USB-пристроїв, а також обізнаність користувачів щодо можливих ризиків та методів захисту. Розвиток нових технологій і методів аутентифікації також відіграє ключову роль у забезпеченні безпеки від цієї нової загрози.

Ключові слова: BadUSB, BushBanny, flash-накопичувач, LANTurtle, RubberDucky, USB пристрій, атака, вразливість, загроза, метод захисту, хост.

KORCHYNSKYI Volodymyr, TARASENKO Iryna,
BIELOVA Iuliia, RATSYBORYNSKYI Serhii, AKAIEV Oleksandr
State University of Intellectual Technologies and Communications

BADUSB-BASED ATTACKS

This paper discusses the general principles of the BadUSB-based attack. This attack exploits vulnerabilities in USB devices to infiltrate malware and attack computer systems. The BadUSB concept is based on modifying the USB device controller software, allowing attackers to change the functionality of the device. For example, to simulate different types of devices, such as a keyboard, mouse, network adapter, etc., to perform various malicious actions. Attackers/hackers can use BadUSB to run malicious code on a host computer. This allows for data interception, remote control, malicious commands, and other malicious operations on the infected system. The BadUSB attack can be used to carry out a wide range of attacks, bypassing traditional security methods. One of the main methods of protecting against BadUSB attacks is to restrict access to USB ports and use access control mechanisms for devices that are connected to the computer. It is also important to keep USB devices' software up to date. To reduce the risks, it is necessary to constantly update security systems and implement control measures to prevent possible attacks via the USB interface. BadUSB is defined as a threat that requires attention and further research to develop more effective methods of detecting and protecting against such attacks while maintaining the functionality of USB devices. However, BadUSB is not limited to imitating peripherals. There are known cases of this attack targeting USB drives and other devices that use a USB connection. Attackers/hackers can insert malicious code or patch software on these devices to perform attacks aimed at stealing or deleting

confidential information. Protecting against BadUSB requires a comprehensive approach, including improving the hardware and software security of USB devices, as well as user awareness of possible risks and protection methods. The development of new technologies and authentication methods also plays a key role in providing security against this new threat.

Keywords: BadUSB, BushBanny, flash drive, LANTurtle, RubberDucky, USB device, attack, vulnerability, threat, protection method, host.

Постановка проблеми у загальному вигляді
та її зв'язок із важливими науковими чи практичними завданнями

Для сучасного світу характерна тенденція збільшення комп'ютерних вірусів, що потребує додаткових зусиль для їх запобігання. Існує велика кількість наукових праць [1,2], що спрямовані на вирішення цих проблем, проте, слід відзначити, що передбачити нові види загроз практично неможливо. З цього приводу перспективним є дослідження нових видів загроз, до яких можна віднести BadUSB атаки. Цей метод включає в себе перепрограмування USB-пристрою таким чином, щоб він визначався комп'ютером як інше обладнання. BadUSB відноситься до класу хакерських атак, що засновані на вразливостях USB-пристроїв [3]. Через відсутність захисту від перепрограмування, реалізація BadUSB атаки може змінити алгоритм роботи USB-пристрою, що дозволяє імітувати роботу іншого обладнання. Таким чином, BadUSB атака призначена для доставки та впровадження шкідливого програмного коду в операційну систему.

Аналіз досліджень та публікацій

Актуальність даної статті обґрунтована необхідністю створення для робочих станцій та серверного обладнання систем захисту від атак, пов'язаних з BadUSB. Офіційно така вразливість була описана у 2014 році, але перші згадки про подібну атаку були ще у 2010 році [3,4].

У вересні 2010 року було виявлено вірус Stuxnet, за допомогою якого була реалізована атака на основі BadUSB [4]. Цей вірус завдав серйозну шкоду та зірвав запуск атомної електростанції (АЕС). Слід відзначити, що системи автоматизованого керування АЕС не були підключені до мережі Інтернет, що робило неможливим втручання ззовні. Проте, вразливість операційної системи та людський фактор дозволив Stuxnet вразити 1368 з 5000 центрифуг, які використовувалися для збагачення урану. Виконавцем цього інциденту став співробітник, який підключив інфікований flash-накопичувач у робочу станцію [5,6].

Станом на 2023 рік не існує дієвих програмних методів захисту від цих атак. У роботі розглянуто можливі шляхи розповсюдження вірусу та способи щодо запобігання цим атакам [7,8]. Таким чином, темою роботи є визначення основних алгоритмів реалізації атак на основі BadUSB та розробка відповідних рекомендацій протидії.

Потенційними «жертвами» від реалізації BadUSB атаки можуть бути комерційні, державні та інші компанії/підприємства, які для роботи використовують робочі станції та/або сервери. Вперше про поняття BadUSB стало відомо від компанії «Security Research Labs» на конференції «BlackHat USA 2014» у серпні 2014 року [4].

Дослідження вразливості комп'ютерних систем на основі BadUSB атаки

Розглянемо вразливості на основі BadUSB атаки. Як правило, USB пристрої мають серед своїх компонентів мікроконтролер, одна із функцій якого є зв'язок із хостом за допомогою USB інтерфейсу. Під час ініціалізації з'єднання мікроконтролер передає хосту дані та службову інформацію класу пристрою. На основі даних, які було передано мікроконтролером, хост завантажує необхідне програмне забезпечення та працює з пристроєм цього класу. При цьому, один USB інтерфейс може обслуговувати одразу декілька класів окремих пристроїв [2].

Вразливість BadUSB виникає через відсутність механізму захисту від перепрограмування USB пристроїв, а в хостах не запроваджена функціональна можливість їх перевірки на автентичність. Через такі недоліки хакери/зловмисники мають змогу змінити внутрішню програму мікроконтролера USB пристрою та здійснити імітацію роботи іншого обладнання. Також, через наявність зв'язку з мікроконтролером, хакер/зловмисник може робити підміну та перехоплення будь-яких даних та команд між USB пристроєм та хостом [3].

Кожний контролер USB є унікальним пристроєм, тому для кожного з них необхідно створювати окремий заражений патч, оскільки неможливо написати універсальне програмне забезпечення та використовувати його на усіх мікроконтролерах USB. Процедура перепрограмування відрізняється в залежності від мікроконтролера USB, тому це значно зменшує ймовірність «епідемії» BadUSB, але не захищає від цілеспрямованої атаки.

Зловмисник, який має змогу вносити зміни у внутрішню програму мікроконтролера USB-пристрою, може зробити такий носій потужним засобом атаки. Зміна програми мікроконтролера дає можливість реалізовувати різні сценарії зараження комп'ютерних систем. USB-пристрій зі шкідливою програмою після

підключення до цільового комп'ютера може інфікувати вбудовані пристрої, що підключаються через порт USB. Після цього заражений комп'ютер інфікує усі накопичувачі, принтери, веб-камери тощо.

Визначимо наступні BadUSB атаки, що можуть використовуватись хакерами/зловмисниками через вразливості USB пристроїв [5,9,10]:

– USB-Killer. Цей пристрій (рис.1), який схожий на звичайний flash-накопичувач, має можливість виводити з ладу материнські плати. Коли USB-Killer підключають до USB-порту цільової машини, починається зарядка його конденсаторів від живлення USB. Після зарядки пристрій розряджає близько «–200В» постійного струму на кола живлення комп'ютера «жертви», при цьому від'ємний струм подається на інформаційні контакти USB-порту через польовий транзистор. Цикл заряджання-розряджання повторюється декілька разів на секунду, поки пристрій USB-Killer не буде вилучено з порту. Таким чином, даний процес ініціює значне перевищення номінальної напруги 5В, що викликає перенавантаження та пошкодження електронних компонентів комп'ютера.

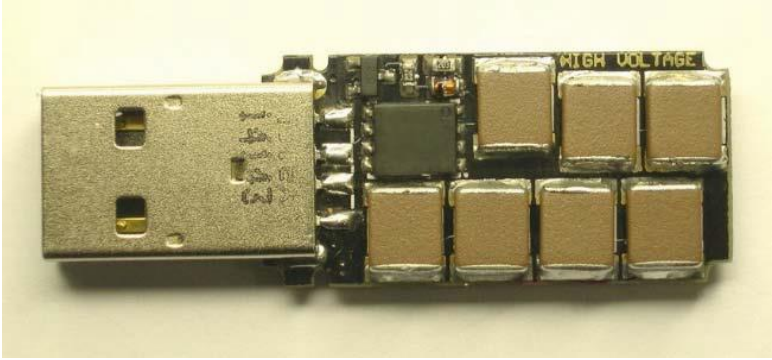

Рис. 1. Пристрій USB Killer

– Імітація клавіатури. Для імітації клавіатури використовується пристрій, який має назву RubberDucky або BushBanny (рис. 2,3). Цей пристрій імітує роботу клавіатури на комп'ютері, а через певний час відправляє зловмиснику послідовність натискання клавіш. Подібні пристрої можуть завантажити та запустити бекдор (програма віддаленого доступу) протягом 30 секунд. Це дає можливість зловмиснику виконувати на атакованому комп'ютері будь-які дії. У якості таких шкідливих пристроїв також може виступати звичайний смартфон на базі операційної системи Android.

Розглянемо технічні характеристики даного пристрою. Цей пристрій реалізовано на основі плати Arduino (рис. 4) з мікропроцесором 60 МГц 32-біт, що дозволяє здійснювати введення команд зі швидкістю до 1000 символів за хвилину. Пристрій має простий синтаксис написання скрипту та легко програмується. Це дає можливість створювати будь-які типи сценаріїв ураження цільового комп'ютера.

Рис. 2. Пристрій BashBunny

Рис. 3. Пристрій RubberDucky

Рис. 4. Пристрій AtMega 32U4

Іншим варіантом реалізації пристрою RubberDucky є використання модулю Wi-Fi (рис. 5), за допомогою якого зловмисник має змогу віддалено виконувати команди. Цей модуль побудовано на основі мікроконтролеру ATMEGA та ESPB266MOD. Такі пристрої дають змогу зловмисникам/хакерам одразу почати створення корисного навантаження та користуватися вразливістю BadUSB.

Рис. 5. Пристрій RubberDucky на основі плати з мікроконтролером AtMega 32U4 з Wi-Fi модулем

– Імітація мережевої карти. Для імітації мережевої карти, використовується пристрій, який імітує роботу мережевої карти комп'ютера (рис. 6). Реалізація цієї загрози дає повний доступ до вхідного/вихідного трафіку, тому за допомогою такого пристрою можна перехоплювати або перенаправляти мережевий трафік. Даний різновид атаки можливий через те, що операційна система комп'ютера автоматично виконує запит DHCP під час розпізнавання нової мережевої карти. При підключенні пристрою LAN Turtle призначається нова IP-адреса комп'ютеру, що дає можливість перехоплювати увесь його трафік. Після цього, коли інфікований комп'ютер відправляє пакет на будь-яку IP-адресу, він буде проходити через шкідливий пристрій USB-Ethernet.

Окрім усього вищеописаного, Ethernet-пристрій LAN Turtle має змогу перехоплювати cookies веб-браузера. Пристрій очікує, коли одна із вкладок здійснить HTTP-запит, а потім зробить підробку відповіді. Після отримання підробленої відповіді веб-браузер на цільовому комп'ютері буде відкривати приховані Iframe'и. У результаті cookies буде перехоплено зловмисником/хакером.

Також Iframe'и, які було описано в попередньому абзаці, можуть завантажити на цільовий комп'ютер шкідливий HTML та JavaScript-код, який потрапляє в кеш, а потім виконує функції бекдору. Зловмисник/хакер може використати це, щоб у подальшому «змусити» комп'ютер звернутися до серверу зі шкідливим програмним забезпеченням для продовження атаки.

Рис. 6. Ethernet-пристрій LAN Turtle

Окрім того, LANTurtle має можливість атакувати роутер, до якого під'єднано цільовий комп'ютер. Пристрій встановлює на нього бекдор і робить комп'ютер доступним із мережі Інтернет, використовуючи DNS rebinding і WebSocket. У результаті зловмисник/хакер може набрати певну URL-адресу і отримати доступ до панелі керування маршрутизатором, що дасть змогу змінити його налаштування, а також перехоплювати/змінювати незашифрований трафік.

– Boot Injection. Для атаки у якості пристрою, який заражає комп'ютер, виступає звичайний USB флеш-накопичувач. Цей пристрій здатний визначити час увімкнення комп'ютера і в момент визначення BIOS'ом запустити вірус для зараження операційної системи. Це стає можливим через те, що «поведінкою» хоста при «спілкуванні» з USB-мікроконтролером можна визначити тип операційної системи та тип BIOS'у.

– Вихід з віртуального оточення. У даному випадку атака завжди використовує можливість повторної ініціалізації пристрою. Вірус виконується на віртуальній машині та заражає будь-який пристрій підключений по USB. Далі виконується нова ініціалізація, яка виступає двома окремими пристроями – новим та попереднім, яке вже було підключене до віртуальної машини.

У результаті атак з використанням «модифікованих» USB-пристроїв існує потенційна можливість приховано отримати керування комп'ютером, здійснювати доступ до інформації, що зберігається на його носіях, відстежувати дії користувача, перехоплювати паролі доступу на PIN-коди, а найголовніше – впровадити вірус у завантажувальний сектор та/або виконувані файли [8,9].

Програмні способи захисту від атак BadUSB засновано на неможливості перепрограмування мікроконтролера та перевірки цілісності хеш-результату внутрішньої програми мікроконтролера. Щодо неможливості перепрограмування мікроконтролеру – це задача виробників мікроконтролерів [4].

Одним з можливих програмних способів захисту комп'ютерів/серверів на підприємстві є програмне обмеження підключення периферійних пристроїв. Проте варто зазначити, що це не може забезпечити повноцінний захист, оскільки BadUSB атаки засновані на тому, що оновлення USB-пристроїв не потребує наявності електронного підпису. Як правило, у таких пристроях відсутня перевірка цілісності підпису виробника [2]. Якщо при модифікації програми проводиться така перевірка, то пристрій з інфікованим програмним забезпеченням не пройде авторизацію. Але станом на зараз деякі виробники уже випускають flash-накопичувачі із системою криптографічного захисту, яка перешкоджає нелегальному запису вбудованого програмного забезпечення.

Фізичними способами захисту від атаки BadUSB, а саме від USB-Killer є використання захисного пристрою, який представлено на рис. 7. Даний пристрій має назву USB-блокер або USB-фільтр, який запобігає пошкодженню від атаки USB-Killer. Даний девайс фільтрує вхідну напругу і захищає комп'ютер. При підключенні USB-Killer через нього він вийде з ладу та збереже материнську плату з усіма електронними компонентами [10].

Рис. 7. USB-блокер

Висновки з даного дослідження і перспективи подальшого розвитку у даному напрямі

Проведено аналіз можливих загроз на основі атаки BadUSB. З'ясовано, що відсутність дієвих механізмів надійного захисту від атаки BadUSB суттєво послаблює систему захисту інформації в комп'ютерних системах. Визначено, що дана атака може приймати різні алгоритми шкідливих дій, включаючи імітацію периферійних пристроїв, таких як клавіатура чи миша, або вплив на USB-накопичувачі та інші підключені пристрої. Причиною того, що зловмисники/хакери мають можливість виконувати дану атаку є відсутність відповідних механізмів захисту від перепрограмування мікроконтролерів USB пристроїв та їх перевірки на автентичність. Саме це дає змогу вносити зміни у внутрішню програму мікроконтролера та реалізовувати різні сценарії зараження комп'ютерних систем. Програмні методи запобігання цих атак

існують, але їх можливо реалізувати лише виробниками мікроконтролерів USB пристроїв, щодо апаратних методів – використання USB-блокеру, який може захистити комп'ютер від USB-killer'а. Також важливою частиною стратегії запобігання цим атакам є використання нових технологій та методів аутентифікації.

Література

1. Make Your Own Bad USB [Електронний ресурс] – Режим доступу до ресурсу: https://null-byte.wonderhowto.com/how-to/make-your-own-bad-usb-0165419/.
2. Scott E. How to Make a Malicious USB Device and Have Some Harmless Fun [Електронний ресурс] / Eggimann Scott. – 2022. – Режим доступу до ресурсу: https://hackernoon.com/how-to-make-a-malicious-usb-device-and-have-some-harmless-fun.
3. Жуков А. Turning a Regular USB Flash Drive into a USB Rubber Ducky [Електронний ресурс] / Антон Жуков – Режим доступу до ресурсу: https://hackmag.com/security/rubber-ducky/.
4. Karsten N. BadUSB - On Accessories that Turn Evil by Karsten Nohl + Jakob Lell [Електронний ресурс] / N. Karsten, L. Jakob. – 2014. – Режим доступу до ресурсу: https://www.youtube.com/watch?v=nuruzFqMgIw.
5. What is Rubber Ducky & Bad Usb [Електронний ресурс] – 2021. – Режим доступу до ресурсу: https://medium.com/@alperenaga/bad-usb-5a0cd2790e09 .
6. Mimoso M. Release of Attack Code Raises Stakes for USB Security [Електронний ресурс] / Michael Mimoso. – 2014. – Режим доступу до ресурсу: https://threatpost.com/badusb-attack-code-publicly-disclosed/108663/.
7. BadUSB Uncovered [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: https://www.wibu.com/ru/press-relizy/detalnaja-informacija-o-press-relizakh/detail/badusb-uncovered.html.
8. USB peripherals can turn against their users [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: https://www.srlabs.de/blog-post/usb-peripherals-turn.
9. Voronova A. Is Your USB-C Dock Out To Hack You? [Електронний ресурс] / Arya Voronova. – 2023. – Режим доступу до ресурсу: https://hackaday.com/tag/badusb/.
10. Rithesh R. An Introduction to The BadUSB Attacks [Електронний ресурс] / Raghavan Rithesh. – 2020. – Режим доступу до ресурсу: https://acodez.in/badusb-attack/.

References

1. Make Your Own Bad USB [Electronic resource] – Mode of access to the resource: https://null-byte.wonderhowto.com/how-to/make-your-own-bad-usb-0165419/.
2. Scott E. How to Make a Malicious USB Device and Have Some Harmless Fun [Electronic resource] / Eggimann Scott. – 2022. – Mode of access to the resource: https://hackernoon.com/how-to-make-a-malicious-usb-device-and-have-some-harmless-fun.
3. Zhukov A. Turning a Regular USB Flash Drive into a USB Rubber Ducky [Electronic resource] / Anthon Zhukov – Mode of access to the resource: https://hackmag.com/security/rubber-ducky/.
4. Karsten N. BadUSB - On Accessories that Turn Evil by Karsten Nohl + Jakob Lell [Electronic resource] / N. Karsten, L. Jakob. – 2014. – Mode of access to the resource: https://www.youtube.com/watch?v=nuruzFqMgIw.
5. What is Rubber Ducky & Bad Usb [Electronic resource] – 2021. – Mode of access to the resource: https://medium.com/@alperenaga/bad-usb-5a0cd2790e09 .
6. Mimoso M. Release of Attack Code Raises Stakes for USB Security [Electronic resource] / Michael Mimoso. – 2014. – Mode of access to the resource: https://threatpost.com/badusb-attack-code-publicly-disclosed/108663/.
7. BadUSB Uncovered [Electronic resource] – 2014. – Mode of access to the resource: https://www.wibu.com/ru/press-relizy/detalnaja-informacija-o-press-relizakh/detail/badusb-uncovered.html.
8. USB peripherals can turn against their users [Electronic resource]. – 2014. – Mode of access to the resource: https://www.srlabs.de/blog-post/usb-peripherals-turn.
9. Voronova A. Is Your USB-C Dock Out To Hack You? [Електронний ресурс] / Arya Voronova. – 2023. – Режим доступу до ресурсу: https://hackaday.com/tag/badusb/.
10. Rithesh R. An Introduction to The BadUSB Attacks [Електронний ресурс] / Raghavan Rithesh. – 2020. – Режим доступу до ресурсу: https://acodez.in/badusb-attack/.